Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3098

Vragen van de leden **Verhoeven** en **Pia Dijkstra** (beiden D66) aan de Ministers van Volksgezondheid, Welzijn en Sport en van Veiligheid en Justitie over *het bericht «Cyber security van apparatuur in ziekenhuizen kwetsbaar»* (ingezonden 3 juni 2016).

Antwoord van Minister **Schippers** (Volksgezondheid, Welzijn en Sport), mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 7 juli 2016) Zie ook Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 2898.

Vraag 1
Bent u bekend met het bericht «Cyber security van apparatuur in ziekenhuizen kwetsbaar»?[1]

Antwoord 1
Ja

Vraag 2
In hoeverre zijn er bij u besmettingsgevallen met malware bij Nederlandse ziekenhuizen bekend?

Antwoord 2
Bij de Inspectie voor de Gezondheidszorg (IGZ) zijn geen concrete meldingen van cyber incidenten bekend. Bij het Nationaal Cyber Security Centrum (NCSC) zijn er in het afgelopen jaar twee vrijwillige meldingen van malware besmettingen geweest. Zoals eerder aangegeven in de beantwoording van vragen van de leden Pia Dijkstra en Kees Verhoeven (d.d. 11 mei 2016) betreffen deze meldingen aanvallen op kantoorautomatisering en zijn er bij het NCSC geen signalen bekend dat deze aanvallen hebben geresulteerd in grootschalige uitval of verstoring.

Vraag 3
Herinnert u zich uw antwoorden op eerdere vragen, waarin u zei dat «het de eigen verantwoordelijkheid van ziekenhuizen is om de informatiebeveiliging op orde te hebben»? Kunnen ziekenhuizen de expertise van het Nationaal

[1] http://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-security-van-apparatuur-in-ziekenhuizen-kwetsbaar.html

ah-tk-20152016-3098
ISSN 0921 - 7398
’s-Gravenhage 2016

Cyber Security Centrum (NCSC) inroepen om hun informatiebeveiliging op orde te krijgen? Zo nee, waarom niet?[2]

Antwoord 3
Ja
In eerdere beantwoording is aangegeven dat informatiebeveiliging een eigen verantwoordelijkheid van de zorginstelling is, ongeacht de mate van ondersteuning die het NCSC een partij biedt. In de EU richtlijn inzake Netwerk- en Informatiebeveiliging (NIB) wordt de zorgsector overigens wel aangewezen als sector waarbinnen moet worden bepaald welke specifieke organisaties aanbieders van essentiële diensten zijn en in verband hiermee onder bepaling van de richtlijn komen te vallen. Over de implementatie van de NIB-richtlijn en verdere acties wordt de Tweede Kamer door de Minister van Veiligheid en Justitie geïnformeerd.
Er is sprake van een omvangrijk aantal activiteiten op het gebied van cybersecurity in de zorg, die met betrokkenheid van het NCSC, worden ontplooid. Allereerst heeft het NCSC in samenwerking met de sector een Information Sharing and Analysis Centre (ISAC) voor de zorg opgezet. Een ISAC is een publiek-privaat sectoraal samenwerkingsverband, waarbinnen op tactisch niveau deelnemers van verschillende ziekenhuizen onderling informatie en ervaringen uitwisselen over cybersecurity en kwetsbaarheden in de sector («situational awareness»).
Daarnaast wordt gewerkt aan de inrichting van een Computer Emergency Response Team (CERT) voor de zorg (Z-CERT). Tot slot publiceert het NCSC openbare kennisproducten (o.a. het Cybersecurity Beeld Nederland (CSBN) en Factsheets) die zorginstellingen kunnen gebruiken bij het verbeteren van hun informatiebeveiliging.
Binnenkort verschijnt ook de tweede druk van het «Convenant Veilige toepassing van medische technologie». Het convenant is een veldnorm voor de instellingen voor medisch-specialistische zorg en biedt handvatten voor de totale levenscyclus van een medisch hulpmiddel. Daarin wordt het aspect «cybersecurity» aangemerkt als onderdeel van de risicoanalyse.

Vraag 4
Bent u bereid onderzoek te doen onder Nederlandse ziekenhuizen en andere zorginstellingen, naar het voldoen van apparatuur aan de privacyregelgeving, het gebruikmaken van versleutelde verbindingen bij op het netwerk aangesloten apparaten en beleid rondom het dichten van kwetsbaarheden in software van medische apparatuur?

Antwoord 4
Informatiebeveiliging is een eigen verantwoordelijkheid van een zorginstelling. De NEN 7510 (en NEN 7512) – waar de ziekenhuizen nu al aan moeten voldoen – geven allerlei technische en organisatorische normen hoe informatiebeveiliging en privacy kan worden bereikt. Deze normen zijn zowel gericht op het voorkómen van incidenten als op het voorbereid zijn wanneer ze optreden. Ziekenhuizen zullen zelf moeten nagaan of nieuwe apparatuur voldoet aan de beveiligingseisen die in deze normen zijn gesteld. Ziekenhuizen kunnen hun informatiebeveiligingsbeleid en de beveiligingsmaatregelen ook periodiek laten auditen.
Informatiebeveiliging van medische hulpmiddelen, waaronder medische apparatuur, maakt deel uit van het ontwikkel (design) proces. In de essentiële eisen die de huidige Europese Medische Hulpmiddelen Richtlijn voorschrijft staat dit weliswaar nog niet expliciet zo genoemd, maar in de tekst van de aankomende verordening wel. Onder Nederlands Voorzitterschap is op 15 juni jl. over deze verordening politiek akkoord bereikt.
De IGZ ziet toe op de naleving van relevante wet- en regelgeving op het gebied van informatiebeveiliging in de zorg, voor zover die raakt aan kwaliteit en veiligheid van zorg. Het genoemde convenant bij het antwoord op vraag 3 valt hier ook onder.
In het Algemeen Overleg van woensdag 29 juni heb ik de TK geïnformeerd over mijn aangekondigde onderzoek, een quickscan, dat ik uitvoer naar de praktijk rond de privacybescherming en omgang met informatiebeveiliging in

[2] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 2512

de ziekenhuizen en GGZ-instellingen. Hierin zal ik onder meer kijken naar de omgang met medische gegevens, de vindbaar- en toegankelijkheid daarvan en voor wie, hoe groot de rol is die privacy en informatiebeveiliging speelt in de eigen dienstverlening en bij uitbesteding van bijvoorbeeld het digitaliseren van patiëntendossiers, of er in de instelling specifiek mensen zijn die verantwoordelijk zijn voor de informatiebeveiliging en hoe deze verantwoordelijkheid is belegd in de Raad van Bestuur en of er geoefend wordt in de organisatie met informatiebeveiligingsincidenten (bijvoorbeeld een hack).

Vraag 5
Deelt u de mening dat de maatschappelijke acceptatie van medische innovaties afhangt van het vertrouwen dat patiënten hebben in de (cyber)-veiligheid van het apparaat en de veilige omgang met gegenereerde (persoons)gegevens? Zo ja, op welke manier draagt u daaraan bij? Zo nee, waarom niet?

Antwoord 5
Veiligheid van medische hulpmiddelen is een belangrijke voorwaarde voor het gebruik. Medische hulpmiddelen dienen, voordat zij tot de markt worden toegelaten, beoordeeld te worden om te bepalen of zij geproduceerd zijn conform de essentiële eisen van de Europese Medische Hulpmiddelen Richtlijn. Cyberveiligheid vormt een groeiend onderdeel van deze beoordeling, gezien de toegenomen verbondenheid van medische apparatuur met de lokale zorginformatiesystemen en de data die deze apparaten verzamelen en verwerken. Er wordt veelal gewerkt volgens de privacy en security by design principes[3], waarbij de apparaten niet zonder reden verbonden zijn met openbare netwerken en data niet zonder reden beschikbaar wordt gesteld aan anderen. De beoordeling en certificering van medische hulpmiddelen gebeurt aan de hand van internationale normen, waarin privacy en cyberveiligheid ook meegenomen worden.
Er is een groeiend bewustzijn rondom de risico's van de steeds meer verbonden medische apparaten. Tevens wordt gewerkt aan het vergroten van het risicobewustzijn bij zorgverleners en instellingen op het gebied van cyberveiligheid en privacy. Zo heeft de Nederlandse Vereniging van Ziekenhuizen (NVZ) een Netwerk Informatiebeveiliging waar kennis en ervaring wordt uitgewisseld, is er een 4-daagse cursus informatieveiligheid ontwikkeld en wordt dit jaar voor het zesde jaar een bewustwordingsweek georganiseerd waar zorgverleners in ziekenhuizen worden gewezen op de risico's van cyberveiligheid en privacy, en de maatregelen die zij daartegen kunnen nemen. Voor meer informatie daarover verwijs ik u naar http://www.zorgzekeren.nl/. Ik steun dit initiatief van harte.

Vraag 6
Bent u bereid, gezien het belang van medische innovaties voor de kwaliteit van de zorg, om een landelijke aanpak te organiseren om de cyber veiligheid van ziekenhuizen en andere zorginstellingen te verbeteren? Zo nee, waarom niet?

Antwoord 6
De eerder genoemde Z-CERT is een landelijk georganiseerde aanpak om cyberveiligheid in de ziekenhuizen te verhogen. De ISAC, heeft eveneens als doel om de cyberveiligheid door de uitwisseling van kennis en informatie te verhogen en is reeds landelijk georganiseerd.
Daarnaast zal ik, zoals eerder ook al in antwoorden op Kamervragen heb aangegeven, met de leden van het Informatieberaad (ondermeer de zorgkoepels, Vereniging Nederlandse Gemeenten, Zorgverzekeraars Nederland) bespreken of het noodzakelijk is om aanvullende maatregelen te nemen

[3] «Privacy by design» houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: «u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.» (definitie AP). In analogie op bovenstaande, wordt bij «Security by design» bij de ontwikkeling al voldoende aandacht besteed aan de informatiebeveiliging(requirements en oplossingen).

om extra waarborgen te realiseren en «privacy en security by design[4]» te stimuleren.
Tot slot verwijs ik naar het aangekondigde onderzoek, een quickscan, rond de privacybescherming en omgang met informatiebeveiliging binnen de ziekenhuizen en GGZ-instellingen, waarover ik u voor eind van dit jaar informeer. Ik zal aan de hand van de bevindingen bezien wat nog extra nodig is.

[4] «Privacy by design» houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: «u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.» (definitie AP). In analogie op bovenstaande, wordt bij «Security by design» bij de ontwikkeling al voldoende aandacht besteed aan de informatiebeveiliging(requirements en oplossingen).